·论著·

图像类医疗大数据隐私加密技术方案及政策立法的协同策略研究

陈开元[1，2]，陈龙[3]，张怡[1，2]，柴润祺[3]，王娜[2]，曾华堂[1，2，4]，柴森春[3*]，梁万年[1，2*]

1.100084 北京市，清华大学万科公共卫生与健康学院
2.100084 北京市，清华大学健康中国研究院
3.100081 北京市，北京理工大学自动化学院
4.518028 深圳市卫生健康发展研究和数据管理中心
*通信作者：柴森春，教授/博士生导师；E-mail：chaisc97@bit.edu.cn
梁万年，教授/博士生导师；E-mail：liangwn@tsinghua.edu.cn
注：陈开元与陈龙为共同第一作者

【摘要】 **背景** 针对图像类医疗大数据隐私加密需求，构建一种创新的基于编码的隐私保护分割技术框架，并从技术与政策立法协同的角度探索促进该技术落地应用的实施路径具有重要意义。**目的** 构建适用于图像类医疗大数据的隐私保护技术框架，提出促进技术应用的政策立法协同策略，以期通过技术创新与政策支持共同推动健康信息化服务体系的完善。**方法** 通过文献综述、理论分析、技术框架构建、实验验证、政策分析等方法构建创新型图像类医疗大数据隐私保护分割技术框架，提出政策立法协同策略。**结果** 成功构建创新型图像类医疗大数据隐私保护分割技术框架并通过有效性验证；针对现行法律法规在云数据处理、责任归属、技术标准及特殊数据保护等方面的不足提出了政策立法建议。**结论** 基于编码的创新型图像类医疗大数据隐私保护分割技术框架能够在保障患者隐私的前提下实现图像类医疗数据的有效共享与利用，提高数据安全性和隐私保护水平；相应政策立法协同策略的提出为图像类医疗大数据的安全治理提供了新思路和新方法。

【关键词】 医疗成像；大数据；数据管理；健康信息互操作性；隐私权；数据加密；政策制订

【中图分类号】 R 446.9 R 197.3 【文献标识码】 A DOI：10.12114/j.issn.1007-9572.2023.0897

Research on the Privacy-Preserving Technical Scheme and the Coordinative Policies Strategies for Big Data in Medical Imaging

CHEN Kaiyuan[1，2]，*CHEN Long*[3]，*ZHANG Yi*[1，2]，*CHAI Runqi*[3]，*WANG Na*[2]，*ZENG Huatang*[1，2，4]，*CHAI Senchun*[3*]，*LIANG Wannian*[1，2*]

1.Vanke School of Public Health，Tsinghua University，Beijing 10084，China
2.Healthy China Research Institute，Tsinghua University，Beijing 10084，China
3.School of Automation，Beijing Institute of Technology，Beijing 100081，China
4.Shenzhen Health Development Research and Data Management Center，Shenzhen 518028，China
**Corresponding author：CHAI Senchun，Professor/Doctoral supervisor；E-mail：chaisc97@bit.edu.cn*
LIANG Wannian，Professor/Doctoral supervisor；E-mail：liangwn@tsinghua.edu.cn

【Abstract】 **Background** Responding to the increasing demand for privacy encryption in image-based medical big data, it is of great importance of proposing an innovative framework of coded-based privacy-preserving segmentation technology, and exploring the implementation pathways to facilitate the practical application of this technology from a collaborative perspective

基金项目：科技创新 2030—“新一代人工智能”重大项目（2021ZD0114100）；深圳市“医疗卫生三名工程”项目（SZSM202111001）

引用本文：陈开元，陈龙，张怡，等.图像类医疗大数据隐私加密技术方案及政策立法的协同策略研究［J］.中国全科医学，2024.［Epub ahead of print］.［www.chinagp.net］

CHEN K Y，CHEN L，ZHANG Y，et al. Research on the privacy-preserving technical scheme and the coordinative policies strategies for big data in medical imaging［J］. Chinese General Practice，2024.［Epub ahead of print］.

of technology and policy legislation. **Objective** To develop a privacy protection technology framework tailored for image-based medical big data, and propose policy and legislative coordination strategies to advance the technology′s adoption, in order to enhance the healthcare informatization service system by combining technological innovation with policy support. **Methods** Construct the innovative framework for privacy preserving segmentation technology in medical image big data by literature review, theoretical analysis, technology framework development, experimental validation, and policy analysis, and then propose the policy and legislative coordination strategies. **Results** We successfully construct the innovative framework for privacy preserving segmentation technology in medical image big data and though the effectiveness verification, and propose specific policy and legislative recommendations addressing the inadequacies of existing laws and regulations in areas such as cloud data processing, liability attribution, technical standards, and special data protection. **Conclusion** Coded-based innovative framework for privacy preserving segmentation technology in medical image big data can enable effective sharing and utilization of image-based medical data by safeguarding patient′s privacy, significantly enhance the data security and privacy protection level, and the proposing of corresponding policy and legislative coordination strategies offers novel insights and approaches to secure governance in this domain.

【Key words】 Medical imaging; Big data; Data management; Health information interoperability; Privacy; Data encryption; Policy making

习近平总书记指出,“创新是一个系统工程,创新链、产业链、资金链、政策链相互交织、相互支撑” “科技创新、制度创新要协同发挥作用,两个轮子一起转”[1],体现了制度协同创新之于科技创新的关键性。2023 年 3 月,中共中央办公厅、国务院办公厅印发《关于进一步完善医疗卫生服务体系的意见》(以下简称《意见》)。为“深入贯彻党中央关于实施健康中国战略的决策部署,推动全面建立中国特色优质高效的医疗卫生服务体系,为人民群众提供全方位全周期健康服务”,《意见》强调发挥信息技术支撑作用,提出“加强健康医疗大数据共享交换与保障体系建设” “推进医疗联合体内信息系统统一运营和互联互通,加强数字化管理” “加快健康医疗数据安全体系建设,强化数据安全监测和预警,提高医疗卫生机构数据安全防护能力,加强对重要信息的保护”等[2],为推进数字健康治理科学化、医疗大数据安全治理领域技术创新等提供了方向指引。

为实现科技创新与制度创新的“双轮驱动”,应切实以制度创新破除制约科技创新的体制机制障碍,通过补齐医疗大数据安全治理领域的规范性、支持性政策立法短板而完善政策协同机制,最大程度上调动创新主体的积极性并释放其创新活力。目前,数字健康治理领域的科学研究在学科交叉融合及技术与政策立法协同方面存在一定的真空地带,导致部分先进技术难以及时落地应用。为积极响应国家战略,探索数字健康治理领域技术方案与政策立法协同机制深度融合路径,本研究以图像类医疗大数据安全治理场景为切入点,深入分析此类场景中隐私加密需求及相关技术研究现状,提出一种基于编码的创新型图像类医疗大数据隐私保护分割技术框架,并从宏观与微观两个层面探索促进图像类医疗大数据隐私加密技术落地应用的政策立法协同策略,以期从科学技术革新与政策立法助力两个维度推动健康信息化服务体系的完善,为健康中国建设献计献策。

1 图像类医疗大数据隐私加密需求及相关技术、政策立法研究现状

随着国家大数据战略的推进与实施,数据的计算与处理逐渐从本地计算机转移至云平台,后者可以在很大程度上解决计算、存储资源及空间问题。在深度学习模型高速发展的背景下,云平台已成为深度学习模型数据库扩容、大数据资源共享及大模型训练的重要依托。在图像类医疗大数据共享交换领域,云服务器的应用是实现不同医疗机构间数据互联互通及跨平台数据分析的主要手段,然而,医疗数据通常包含患者隐私等敏感信息,须通过加密技术等加以保护,在保障有益共享的前提下限制未经授权的数据访问及泄露。如何平衡数据开放与加密的限度并增强共享交换策略的可控性、稳定性是相关技术、政策立法研究共同面临的重要问题。

1.1 相关技术研究现状

在技术层面,过度的医疗数据隐私限制会阻碍不同医疗机构间的合作,因此需积极开发适当的隐私加密算法,以实现数据开放与加密的有效平衡、安全可控。目前,用于实现图像类医疗大数据隐私加密的算法主要包括 4 大类:联邦学习、数据变换、同态加密、可学习的图像加密。此外,部分学者还基于主流框架提出了一些其他类型的隐私加密算法。现阶段主流图像类医疗大数据隐私加密算法及代表性研究详见表 1。

1.2 相关政策立法研究现状

目前,医疗大数据安全治理相关政策立法研究已充分论证了医疗大数据隐私保护的必要性:吕欣等[16]的研究论述了大数据安全和隐私保护的重要价值及关键技术突破在其中发挥的核心作用;闫倩等[17]的研究支持医学数据开放与安全政策协同的必要性;刘军平等[18]

表1 现阶段主流图像类医疗大数据隐私加密算法及代表性研究
Table 1 Current mainstream research on privacy encryption algorithm in the field of big data for medical imaging

隐私加密算法	算法特征	代表性研究
联邦学习	联邦学习采用分布式学习框架，允许不同的数据持有者在不共享原始数据的情况下合作训练强大的模型；只共享梯度和权重等参数，数据本身不发生转移，可有效防止任何潜在的数据泄露；在推理阶段，当使用云服务器时，可能不会阻止来自本地的原始数据传输；局限性：如果网络组织较大，则通信成本较高	（1）用于脑肿瘤图像分割的联邦学习算法[3]；（2）基于联邦学习的多功能磁共振成像分析[4]；（3）用于混合图像标签的医学图像分割[5]
数据变换	数据变换指利用神经网络等方法将原始数据转换为其他形式，从而隐藏其包含的隐私信息；局限性：只保护了推理阶段的隐私，而训练阶段的隐私泄露风险仍然存在	（1）基于特征提取网络的数据变换[6]；（2）基于预训练模型网络层分离的数据转换[7]；（3）基于对抗训练的数据转换[8]
同态加密	同态加密通过对神经网络中的非线性操作进行多项式近似而能够直接使用加密数据进行训练，无需事先解密；局限性：对网络的修改会导致性能下降和计算复杂度增加，难以应用于复杂任务	（1）CryptoNets[9]；（2）CryptoDL[10]
可学习的图像加密	可学习的图像加密指对隐私图像进行加密，加密后的图像仍可应用深度学习方法；局限性：加密后的图像目前仅能用于分类等简单任务，对于分割掩膜等像素简单的图像难以实现加密	（1）提出可学习的图像加密概念[11]；（2）提出改进加密方法，使模型能同时用于加密图像和原始图像[12]；（3）引入参数平衡隐私保护和模型性能[13]
其他	利用生成对抗网络（GAN）从分割掩膜生成图像用于后续训练，从而保证原始图像不被获取；利用GAN混淆患者身份信息，从而实现隐私保护；局限性：分割掩膜信息没有受到保护，分割掩膜信息泄露会使隐私泄露风险大为增加	（1）利用掩膜生成医学图像[14]；（2）利用GAN混淆患者身份[15]

的研究从静态安全和动态安全两个维度阐释了医疗数据安全的内涵和外延，提出应建立医疗数据全生命周期防护体系的建议；叶竹盛等[19]的研究探讨了我国当前法律框架中医疗数据的“去标识化”和“匿名化”制度基础。然而，上述医疗大数据安全治理相关政策立法研究多是基于单一学科理论，未与技术发展、实践有机结合，且研究视角多集中在宏观概念及不同政策之间的耦合关系，缺乏针对有关政策落地方案的探索。

综上，医疗大数据高效治理格局的实现需要从两个方面进行突破：一是不断创新、研发关键技术；二是持续推进技术与政策立法的协同发展。因此，本研究拟突破传统单一学科研究范式，在针对当前技术短板提出改进方案的基础上，深度结合图像类医疗大数据共享交换应用场景具体需求及技术特点，以促进技术落地及制度贯彻为导向，探索切实可行的政策立法支撑方案。

2 图像类医疗大数据隐私加密技术方案

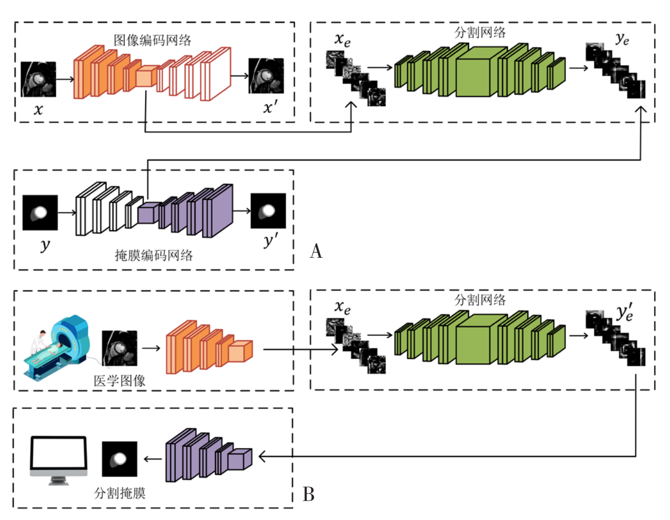
2.1 概述

针对图像类医疗大数据共享交换隐私加密需求，本研究团队提出了一种基于编码的创新型图像类医疗大数据隐私保护分割技术框架，该框架包括部署于客户端的图像编码网络、掩膜编码网络和部署于服务器端的分割网络（图1），可通过对数据编码将数据变换为不包含视觉隐私信息的编码，从而实现原始数据的隐私保护。

2.2 图像/掩膜编码网络

图像编码网络本质上是一个由编码器和解码器组合而成的自动编码器，具有相同的输入和目标。输入或目标通常为MRI图像、X线图像等医疗图像。编码器由1个输入层和4个下采样层组成，其中输入层是1个卷积块的重复应用，包括1个核大小3×3、步幅2、填充1的卷积层，随后是批量归一化（batch normalization，BN），1个线性整流函数（rectified linear unit，ReLU）激活函数层，以稳定训练；下采样层类似于输入层，但在卷积块之前包含一个步幅2的最大池化操作。解码器由4个上采样层和1个输出层组成，其中上采样层利用尺度为2的双线性插值来恢复特征图的分辨率；输出层是1个1×1卷积层，没有填充，以保证输出形状与输入相同。

掩膜编码网络遵循与图像编码网络相同的架构，但具有不同的输入和目标，其中输入被替换为特定任务的



注：A为训练设置，B为推理设置；x表示医学图像，x′表示重建的医学图像，xe表示编码医学图像，ye表示编码分割掩膜，y表示分割掩膜，y′表示重建的分割掩膜，ye′表示预测的编码分割掩膜。

图1 创新型图像类医疗大数据隐私保护分割技术框架

Figure 1 Innovative framework for privacy preserving segmentation technology in medical image big data

金标准分割掩码，目标的通道数被更改为与分割前景类别数一致。一旦图像编码网络训练完成，来自图像编码网络和掩膜编码网络的编码器输出将分别作为分割网络的输入和目标。

图像/掩膜编码网络结构详见表2。

表2 图像/掩膜编码网络结构
Table 2 Image/mask encoding network architecture

构成部分	网络层名	网络层细节	输出大小
编码器	输入层	[Conv，BN，ReLU]×2	（8，H，W）
	下采样层1	Downsampling+[Conv，BN，ReLU]×2	（16，H/2，W/2）
	下采样层2	Downsampling+[Conv，BN，ReLU]×2	（32，H/4，W/4）
	下采样层3	Downsampling+[Conv，BN，ReLU]×2	（64，H/8，W/8）
	下采样层4	Downsampling+[Conv，BN，ReLU]×2	（128，H/16，W/16）
解码器	上采样层4	Upsampling+[Conv，BN，ReLU]×2	（64，H/8，W/8）
	上采样层3	Upsampling+[Conv，BN，ReLU]×2	（32，H/4，W/4）
	上采样层2	Upsampling+[Conv，BN，ReLU]×2	（16，H/2，W/2）
	上采样层1	Upsampling+[Conv，BN，ReLU]×2	（8，H，W）
	输出层	Conv（1×1）	和输入一致

注：Conv=卷积层，BN=批量归一化，ReLU=线性整流函数，H表示图像高度，W表示图像宽度，Downsampling表示下采样操作，Upsampling表示上采样操作

2.3 分割网络

分割网络不同于广泛应用的U型结构分割网络[20]，其通常使用多个下采样操作步骤，并跟随多个上采样操作步骤。分割网络在编码器中采用双线性插值，在卷积层之后的解码器中采用最大池化操作，这就导致中间特征的空间维度大于输入或输出；为了利用全局上下文信息，在靠近输入和输出层的位置采用了金字塔池化模块（PPM）[21]，以融合不同池化尺度下的特征。本研究使用的PPM是1个四层的模块，其池化尺度分别为1、3、5、7。此外，本研究还采用编码器与解码器之间的跳跃连接[22]，以更好地保留位置信息剩余的架构与图像/掩膜编码网络相同。分割网络的输入来自图像编码网络的编码图像，目标来自掩膜编码网络的编码掩码，而由于从图像编码网络中分离出来的编码器的输出已包含了足够的高层语义含义，没必要再冒着丢失更多位置信息的风险通过下采样操作来提取特征，因此本研究的分割网络采用了上述过完备架构。

综上，创新型图像类医疗大数据隐私保护分割技术框架的3个网络是独立的，只要数据准备就绪，就可以在不需要来自其他网络的梯度或特征的情况下进行训练。通常情况下，对于隐私保护分割，创新型图像类医疗大数据隐私保护分割技术框架的图像编码网络和掩膜编码网络部署在医院或医疗实体等客户端，而分割网络则部署在服务器端，即云服务提供商等。

2.4 训练过程和推理过程

训练过程：首先，通过最小化输入和输出之间的差值训练图像编码网络和掩膜编码网络，训练完成后将编码器从编码网络中分离出来，对图像和GT分割掩码进行编码；其次，将包含足够语义信息和很少视觉信息的编码图像和掩码传输到服务器端，以训练分割网络学习编码图像到编码掩码的映射。创新型图像类医疗大数据隐私保护分割技术框架的训练过程见图2。

推理过程：完成3个网络的训练后，创新型图像类医疗大数据隐私保护分割技术框架就可用于医学图像分割，在此阶段，只需要图像编码网络的编码器、掩膜编码网络的解码器和分割网络：首先，由客户端的编码器对医学图像进行编码；其次，将编码后的图像传输到服务器端作为分割网络的输入，然后再将输出传输回客户端；最后，由解码器对从服务器端返回的数据进行解码，从而获得图像的预测分割掩码，实现通过仅传输编码数据同时保留原始图像甚至掩码在本地的方式来保护图像类医疗大数据隐私。创新型图像类医疗大数据隐私保护分割技术框架的推理过程见图3。

2.5 有效性验证

基于公开的心脏MRI数据集（来自多中心、多供应商、多疾病心脏分割挑战赛，共包含320个来自5个医疗中心的具有手工标注的样本并进行了多次实验）[23]前3个医疗中心的数据与Python 3.10、PyTorch 1.12.0、Ubuntu 18.04，以Dice相似系数（dice similarity coefficient，DSC）作为评价指标，验证创新型图像类医疗大数据隐私保护分割技术框架的有效性，结果显示，其在前3个医疗中心数据中的DSC分别为81.14%、80.67%、80.15%，证实了该框架的有效性。

3 图像类医疗大数据隐私保护政策立法的协同机制

创新型图像类医疗大数据隐私保护分割技术框架主

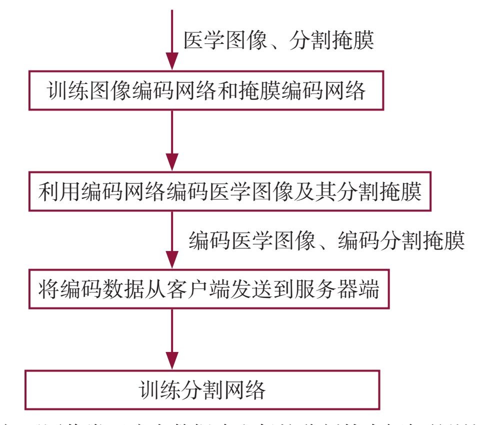


图2 创新型图像类医疗大数据隐私保护分割技术框架的训练过程
Figure 2 Training process of the innovative framework for privacy preserving segmentation technology in medical image big data

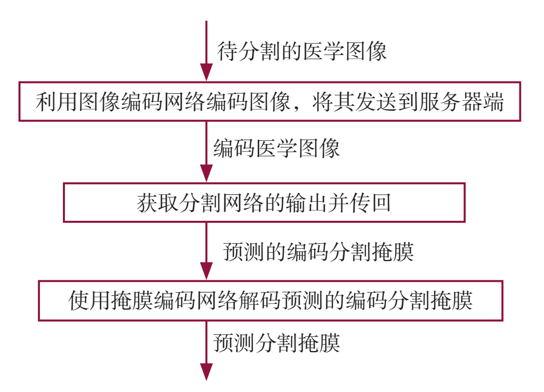


图 3 创新型图像类医疗大数据隐私保护分割技术框架的推理过程
Figure 3 Inference process of the innovative framework for privacy preserving segmentation technology in medical image big data

要分为训练过程和推理过程，数据流转主要在“客户端－云服务器－客户端”这一闭环中进行，其基础架构与当前主流的用于图像类医疗大数据深度学习类隐私加密算法一致。因此，基于创新型图像类医疗大数据隐私保护分割技术框架探讨政策立法在各环节及各主体层面的协同策略具有合理性与普适性，但是，创新型图像类医疗大数据隐私保护分割技术框架下相关数据在云服务器的加密流转是图像类医疗大数据深度学习类隐私加密算法中不可或缺的环节之一，我国现阶段的数据安全治理政策立法对于规范云端数据存在一定缺位，且针对图像类医疗大数据等敏感数据的保护尚存在较大的制度建设空间。

3.1 医疗大数据安全治理政策立法现状及面临的问题

自 2015 年党的十八届五中全会首次提出“国家大数据战略”以来，中共中央、国务院陆续出台了一系列政策、规范文件，逐步建立起较为完备的数据基础制度。2022 年 12 月，中共中央、国务院出台《关于构建数据基础制度更好发挥数据要素作用的意见》[24]，进一步明确了数据基础制度的外延，即数据产权制度、流通交易制度、收益分配制度、安全治理制度，其中数据产权制度、流通交易制度均需以保障数据安全为前提。由此可见，安全治理制度是数据基础制度的核心。然而，由于我国数据安全治理制度建设尚处于起步阶段，顶层架构尚未完全建立健全，因此数据安全治理体系仍存在主责部门不清、相关主体权责界限模糊、跨部门协同未形成制度化、缺乏常态化统筹协调机制等问题，并有赖于相关政策立法的完善。

在数据安全治理方面，我国的顶层法律法规主要包括《中华人民共和国民法典》第四编第六章“隐私与个人信息保护”、《中华人民共和国刑法》中有关数据犯罪的条款及《中华人民共和国网络安全法》《中华人民共和国数据安全法》《中国人民共和国个人信息保护法》《关键信息基础设施安全保护条例》等。在医疗大数据安全治理领域，相关法律法规还包括《中华人民共和国基本医疗卫生与健康促进法》，且《中华人民共和国基本医疗卫生与健康促进法》第四十九条对健康医疗数据安全保障提出了更为具体的要求，包括：“加快医疗卫生信息基础设施建设，制定健康医疗数据采集、存储、分析和应用的技术标准”“推进医疗卫生机构建立健全医疗卫生信息交流和信息安全制度”等。

对于医疗大数据安全治理，上述法律法规面临的问题主要分为 3 个方面：（1）有关数据安全治理的条款多为原则性规定，缺乏实施细则，数据治理主体缺乏有效的制度性参考，无法真正推进数据安全治理工作的落地实施，导致数据安全无法得到有效保障，如《中华人民共和国数据安全法》第三章“数据安全制度”第二十二条虽规定：“国家建立集中统一、高效权威的数据安全风险评估、报告、信息共享、监测预警机制”，但并未对相关机制的主责部门及实施程序作出具体规定。（2）不同层级、不同时间颁布的法律法规在数据保护对象、数据处理者义务等方面的规定存在冲突，导致各主体在开展数据安全治理相关工作时缺乏一致性及有序性，如《中华人民共和国刑法》保护的数据仅包括“计算机信息系统中存储、处理或者传输的数据”，但在《中华人民共和国数据安全法》《中华人民共和国个人信息保护法》中，受保护的数据类型则不限于计算机信息系统中的数据。（3）当前政策立法存在一定的滞后性及碎片化特征，无法完全适应当前技术发展，主要表现为数据安全立法滞后于相关技术及业务发展，多项法规、政策、标准、实施细则未实现体系化整合且存在制度缺位，如现行法律法规未明确云端大数据传输及加密规范，国家层面立法与地方、行业立法在数据开放主管部门、数据标准、个人权利保护程度等方面未实现系统化整合。

上述法律法规在医疗大数据安全治理领域面临的问题一方面会加剧数据孤岛的形成，另一方面可能导致相关大数据新技术业态发展面临无法可依的情况。

需要指出的是，为推动医疗大数据的互联互通，完善相关数据安全治理制度，中共中央、国务院及中央网信办、工业和信息化部、国家卫生健康委员会等部门制定并发布了更具针对性的政策文件，在一定程度上填补了顶层政策立法的不足，相关政策文件主要包括：国务院办公厅于 2016 年印发的《关于促进和规范健康医疗大数据应用发展的指导意见》、于 2018 年印发的《关于促进“互联网＋医疗健康”发展的意见》；国家卫生健康委于 2018 年印发的《国家健康医疗大数据标准、安全和服务管理办法（试行）》和《全国医院信息化建设标准与规范（试行）》，国家卫生健康委、国家中医药管理局于 2019 年印发的《关于落实卫生健康行业网

络信息与数据安全责任的通知》，国家卫生健康委、国家医疗保障局、国家中医药管理局于 2020 年印发的《关于深入推进“互联网 + 医疗健康”“五个一”服务行动的通知》，国家卫生健康委、国家中医药局于 2020 年印发的《关于加强全民健康信息标准化体系建设的意见》，国家卫生健康委、国家中医药局、国家疾控局于 2022 年印发的《“十四五”全民健康信息化规划》等。此外，国家卫生健康委还先后发布了 227 项卫生健康信息化标准，进一步完善了医疗大数据安全治理体系。然而，上述具有针对性的政策文件在顶层设计与贯彻落实方面仍存在一定短板：（1）政策文件的顶层设计未能完全匹配大数据领域的技术发展，如一些新兴类型数据的保护未被政策文件覆盖，数据安全保护技术的合规性尚未得到有关政策文件支持，行业促进性政策文件未提供重点技术鼓励清单等；（2）有关部门尚未对相关政策、标准文件进行系统化梳理并在统一平台公布，上传下达存在一定的不畅；（3）国家相关部门未对地方政府制定的数据治理政策及标准进行全面的合规审查，且未对中央及地方的权力边界进行明确划分，导致中央和地方的政策及标准兼容性较差，一定程度上加剧了医疗大数据治理制度的碎片化。

3.2 基于图像类医疗大数据隐私加密场景的“科技 – 制度”一体化解决方案

在图像类医疗大数据隐私加密场景中，现行法律法规及政策在隐私保护方面尚存在以下问题：（1）同一数据在不同类型终端的流转未被充分考虑，如前所述，《中华人民共和国刑法》保护的数据仅包括“计算机信息系统中存储、处理或者传输的数据”，针对云数据的犯罪如何入刑尚有待相关法律及司法解释进一步明确。（2）相关法律法规及政策不能适应云平台“去中心化”特征，如《中华人民共和国数据安全法》第二十七条规定：“重要数据的处理者应当明确数据安全负责人和管理机构，落实数据安全保护责任”，该条款用于本地数据时具有可执行性，但涉及“去中心化”的云端数据处理时则很难明确责任归属；此外，我国各层级相关政策文件亦未对云端数据隐私保护的责任主体作出统一规定。（3）隐私保护方面尚缺乏相应的技术标准。图像类医疗大数据具有两项基本特征，即图像数据的二维性和医疗数据的敏感性，但现行法律法规及政策文件并未针对不同类别数据制定差异化技术标准，且已有的技术标准的规范对象多为数据元，并未对技术准入标准作出规定。（4）在顶层法律法规层面未充分体现对敏感性医疗数据的特殊保护。有关医疗大数据治理及健康信息保护的法律条款主要见于《中华人民共和国基本医疗卫生与健康促进法》第四十九条、《中华人民共和国个人信息保护法》第二十八条、最高人民法院《关于审理利用信息网络侵害人身权益民事纠纷案件适用法律若干问题的规定》第十二条等，但其实施细则有待进一步明确。由此可见，政策立法与目前主流图像类医疗大数据隐私加密技术存在一定脱节问题，相关技术或可因缺乏制度保障而难以落地。

针对图像类医疗大数据隐私加密场景制定“科技 – 制度”一体化解决方案，首先应明确场景需求、主要技术环节、技术边界及制度短板，进而通过推进制度框架与技术框架的融合而实现二者的协同，具体到本研究微观层面的聚焦点—图像类医疗大数据隐私加密场景而言，其主要场景需求是实现图像类医疗信息在“客户端 – 云服务器端 – 客户端”的“可视化 – 隐私加密 – 数据解码”。因此，制定相关数据治理政策时应充分考虑该场景中数据流转特点，对同一数据的全生命周期可溯源性作出规定，并明确同一数据在不同流转环节中的差异化隐私保护方式、程度及责任归属。此外，由于当前隐私加密算法的主要目的在于促进基于云服务器的医学图像多中心协作，且本研究已验证了创新型图像类医疗大数据隐私保护分割技术框架的有效性，因此可以考虑将“鼓励基于云服务器的医学图像多中心协作”纳入数字健康促进政策。在技术标准制定方面，本研究已对主流图像类医疗大数据隐私加密算法进行了系统梳理，可考虑以此为基础，联合主责部门及业界专家明确隐私加密技术准入指标，并以标准合规审查为目的，通过试点示范方式在推广前预评估相关指标与各类强制性、促进性政策的契合度。

“十四五”规划纲要已明确建设数字中国战略部署，并将加强公共数据开放共享列为重点工作之一，提出“建立健全国家公共数据资源体系，确保公共数据安全，推进数据跨部门、跨层级、跨地区汇聚融合和深度利用”。因此，协同推进图像类医疗大数据共享学习技术、隐私加密技术及数据安全治理制度发展有助于这一战略目标在医疗卫生领域的落地。同时，随着大数据时代科学技术的迭代更新，大数据的类型、承载媒介、处理及传输技术手段等亦呈现多元化发展。因此，以技术应用场景为单元实施“科技 – 制度”一体化解决方案可在最大程度上推动相关制度的与时俱进，但考虑到政策立法稳定性与合理性的平衡，宜在充分、全面考虑医疗大数据领域各类场景需求及技术共性的基础上完善原则性的顶层立法，在实施细则、司法解释、各层级政策及技术标准中充分考虑不同场景需求之间的差异，从宏观与微观、技术与制度等维度完善我国图像类医疗大数据安全治理体系，形成科技与制度相互促进的可持续发展格局。

4 小结与展望

本研究论述了从技术发展及政策立法两个维度“双

管齐下”推进我国医疗大数据安全治理体系发展与完善的重要性，通过聚焦图像类医疗大数据隐私加密场景下的“科技－制度”一体化解决方案，提出促进技术与政策立法高效匹配与协同的可行路径。当前，数字健康领域的各类技术正处于高速发展阶段，政策立法的滞后性问题日益凸显。在技术研发阶段针对新兴技术框架及特点同步开展具有针对性的制度匹配研究或可在一定程度上解决制度的滞后性问题，从而优化科研促进环境，推动新技术的研发与及时落地。在此过程中，探索多学科融合路径并建立创新型交叉学科研究范式至关重要。

作者贡献：陈开元负责研究选题与设计，论文撰写；陈龙负责算法设计、数据处理、计算机代码实现；张怡、柴润祺负责论文修订；王娜、曾华堂负责提供研究数据，参与理论研究；柴森春、梁万年负责选题指导、审阅与修订论文，对文章整体负责。

本文无利益冲突。

陈开元 https://orcid.org/0000-0001-5165-0802

参考文献

［1］李蕾．协同推进科技创新和制度创新［EB/OL］．（2023-12-15）［2024-01-22］．https://politics.gmw.cn/2023-12/15/content_37030655.htm.

［2］新华社．中共中央办公厅 国务院办公厅印发《关于进一步完善医疗卫生服务体系的意见》［EB/OL］．（2023-03-23）［2023-11-13］．https://www.gov.cn/zhengce/2023-03/23/content_5748063.htm.

［3］LI W，MILLETARÌ F，XU D，et al. Privacy-preserving federated brain tumour segmentation［C］. Machine Learning in Medical Imaging：10th International Workshop，MLMI 2019，Held in Conjunction with MICCAI 2019，Shenzhen，China，October 13，2019，Proceedings 10. Springer International Publishing，2019：133-141. DOI：10.1007/978-3-030-32692-0_16.

［4］LI X，GU Y，DVORNEK N，et al. Multi-site fMRI analysis using privacy-preserving federated learning and domain adaptation：ABIDE results［J］. Med Image Anal，2020，65：101765. DOI：10.1016/j.media.2020.101765.

［5］WICAKSANA J，YAN Z，ZHANG D，et al. FedMix：mixed supervised federated learning for medical image segmentation［J］. IEEE Trans Med Imaging，2023，42（7）：1955-1968. DOI：10.1109/TMI.2022.3233405.

［6］LI M，LAI L Z，SUDA N，et al. PrivyNet：A flexible framework for privacy-preserving deep neural network training with a fine-grained privacy control［J］．（2017-09-18）arXiv：1709.06161v1.

［7］OSIA S A，TAHERI A，SHAMSABADI A S，et al. Deep private-feature extraction［C］. IEEE Transactions on Knowledge and Data Engineering，2020，32（1）：54-66. DOI：10.1109/TKDE.2018.2878698.

［8］DING X，FANG H，ZHANG Z，et al. Privacy-preserving feature extraction via adversarial training［C］. IEEE Transactions on Knowledge and Data Engineering，2022，34（4）：1967-1979. DOI：10.1109/TKDE.2020.2997604.

［9］DOWLIN N，GILAD-BACHRACH R，LAINE K，et al. Cryptonets：applying neural networks to encrypted data with high throughput and accuracy［C］. Proceedings of the 33rd International Conference on Machine Learning，New York，USA，2016. DOI：10.1109/RWS.2014.6830099.

［10］HESAMIFARD E，TAKABI H，GHASEMI M. CryptoDL：Deep neural networks over encrypted data［J］．（2017-11-15）arXiv：1711.05189v1.

［11］TANAKA M. Learnable image encryption［C］. 2018 IEEE International Conference on Consumer Electronics-Taiwan（ICCE-TW），Taichung，Taiwan. 2018：1-2. DOI：10.1109/ICCE-China.2018.8448772.

［12］SIRICHOTEDUMRONG W，KINOSHITA Y，KIYA H. Pixel-based image encryption without key management for privacy-preserving deep neural networks［J］. IEEE Access，2019，7：177844-177855. DOI：10.1109/ACCESS.2019.2959017.

［13］HUANG Q X，YAP W L，CHIU M Y，et al. Privacy-preserving deep learning with learnable image encryption on medical images［J］. IEEE Access，2022，10：66345-66355. DOI：10.1109/ACCESS.2022.3185206.

［14］CHANG Q，QU H，ZHANG Y，et al. Synthetic learning：Learn from distributed asynchronized discriminator GAN without sharing medical image data［C］. 2020 IEEE/CVF Conference on Computer Vision and Pattern Recognition（CVPR），Seattle，USA，2020：13853-13863. DOI：10.1109/CVPR42600.2020.01387.

［15］KIM B N，DOLZ J，JODOIN P M，et al. Privacy-net：an adversarial approach for identity-obfuscated segmentation of medical images［J］. IEEE Trans Med Imaging，2021，40（7）：1737-1749. DOI：10.1109/TMI.2021.3065727.

［16］吕欣，韩晓露．健全大数据安全保障体系研究［J］．信息安全研究，2015，1（3）：211-216.

［17］闫倩，马海群．我国开放数据政策与数据安全政策的协同探究［J］．图书馆理论与实践，2018（5）：1-6.

［18］刘军平，黄泽雨．医疗数据安全之困境及其破解路径［J］．医学与法学，2023，15（5）：14-19.

［19］叶竹盛，刘婉君．医疗科研中的生物医疗数据“匿名化”问题研究［J］．医学与法学，2023，15（4）：44-53.

［20］RONNEBERGER O，FISCHER P，BROX T. Invited talk：U-net：Convolutional networks for biomedical image segmentation［C］. Medical Image Computing and Computer-Assisted Intervention-MICCAI 2015：18th International Conference，Munich，Germany，October 5-9，2015，Proceedings，Part Ⅲ 18. Springer International Publishing，2015：234-241.

［21］ZHAO H，SHI J，QI X，et al. Pyramid scene parsing network［C］. 2017 IEEE Conference on Computer Vision and Pattern Recognition（CVPR），Honolulu，USA，2017：6230-6239. DOI：10.1109/CVPR.2017.660.

［22］HE K，ZHANG X，REN S，et al. Deep residual learning for image recognition［C］. 2016 IEEE Conference on Computer Vision and Pattern Recognition（CVPR），Las Vegas，USA，2016：770-778. DOI：10.1109/CVPR.2016.90.

［23］CAMPELLO V M，GKONTRA P，IZQUIERDO C，et al. Multi-

centre，multi-vendor and multi-disease cardiac segmentation：the M&Ms challenge［J］. IEEE Trans Med Imaging，2021，40（12）：3543-3554. DOI：10.1109/TMI.2021.3090082.

［24］新华社 . 中共中央 国务院关于构建数据基础制度更好发挥数据要素作用的意见［EB/OL］.（2022-12-19）［2023-11-14］. https://www.gov.cn/zhengce/2022-12/19/content_5732695.htm.

（收稿日期：2024-04-08；修回日期：2024-09-04）

（本文编辑：鹿飞飞）